

PATENT ABSTRACTS OF JAPAN

(11)Publication number.: 2001-243444

(43)Date of publication of application : 07.09.2001

(51)Int.Cl. G06K 19/10
G06K 17/00
G06K 19/00

(21)Application number : 2000-049950

(71)Applicant : NTT DOCOMO INC

(22)Date of filing : 25.02.2000

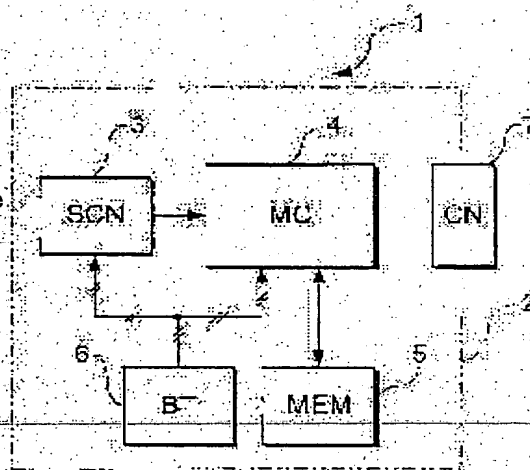
(72)Inventor : FUKUMOTO MASAOKI
SUGIMURA TOSHIKI

(54) PC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To identify a user by making the user grip a PC card before loading the card into external equipment.

SOLUTION: On the housing part 2 of the PC card 1, a grip part that the user grips when loading the housing part 2 into the external equipment is formed and the grip part is provided with an SCN 3 for inputting fingerprint information of the user. A microcontroller 4 identifies the user according to the fingerprint information. Before the PC card 1 is loaded into the external equipment, the PC card 1 is put in a specific operation allowed state or operation disallowed state according to the result of the identification.



LEGAL STATUS

[Date of request for examination]

08.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C), 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-243444

(P2001-243444A)

(43) 公開日 平成13年9月7日(2001.9.7)

(51) Int.Cl.

識別記号

F I

テマコード*(参考)

G 0 6 K 19/10
17/00
19/00

G 0 6 K 17/00
19/00

V 5 B 0 3 5
S 5 B 0 5 8
T

審査請求 未請求 請求項の数 6 O L (全 6 頁)

(21) 出願番号

特願2000-49950(P2000-49950)

(22) 出願日

平成12年2月25日(2000.2.25)

(71) 出願人 392026693

株式会社エヌ・ティ・ティ・ドコモ

東京都千代田区永田町二丁目11番1号

(72) 発明者 福本 雅朗

東京都港区虎ノ門二丁目10番1号 エヌ・

ティ・ティ移動通信網株式会社内

(72) 発明者 杉村 利明

東京都港区虎ノ門二丁目10番1号 エヌ・

ティ・ティ移動通信網株式会社内

(74) 代理人 100098084

弁理士 川▲崎▼ 研二 (外2名)

Fターム(参考) 5B035 AA14 BB09 BC00 CA05 CA38

5B058 CA12 KA02 KA04 KA12 KA38

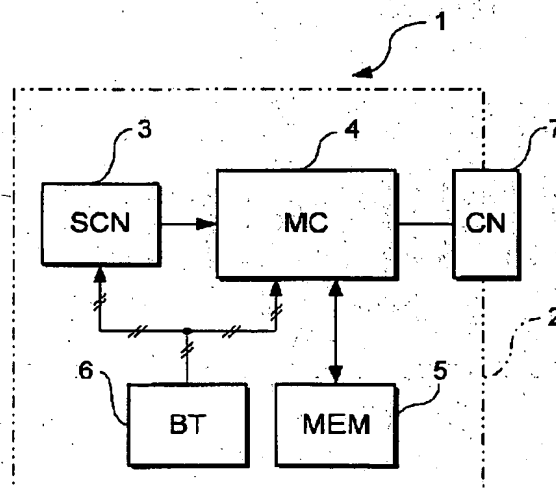
YA20

(54) 【発明の名称】 PCカード

(57) 【要約】

【課題】 外部機器へのカード装着に先立って、使用者がPCカードを把持することにより、本人認証を行う。

【解決手段】 PCカード1の筐体部2には、筐体部2を外部機器に装着する際に使用者に把持される把持部が形成され、この把持部には使用者の指紋情報を入力するSCN9が設けられる。マイクロコントローラ4は、SCN9からの指紋情報に基づいて特定の使用者か否かの認証処理を行う。PCカード1を外部機器に装着する前に、認証処理の結果に基づいて、PCカード1を所定の動作許可状態又は動作禁止状態にする。



【特許請求の範囲】

【請求項1】 外部機器に着脱されるPCカードであって、

コネクタを有する筐体部と、

該筐体部の表面に設けられ、使用者が把持する把持部と、

該把持部を使用者が把持したとき、使用者の生体情報を検出する生体情報検出手段と、

前記生体情報検出手段で検出された生体情報に基づいて特定の使用者か否かの本人認証を行う認証処理手段と、

前記生体情報検出手段及び認証処理手段を駆動するための電力を供給する内蔵電源と、を備えたことを特徴とするPCカード。

【請求項2】 前記筐体部が外部機器に装着されるとき、前記認証処理手段の認証結果に基づいて、当該PCカードを外部機器に対して動作許可状態又は動作禁止状態にすることを特徴とする請求項1に記載のPCカード。

【請求項3】 前記生体情報検出手段は、前記把持部に設けられ、該把持部を把持する使用者の指紋情報を検出することを特徴とする請求項1または2に記載のPCカード。

【請求項4】 請求項1または2に記載のPCカードにおいて、前記認証処理手段による本人認証が完了してから所定時間の間、認証結果を出力することを特徴とするPCカード。

【請求項5】 請求項1～4に記載のPCカードにおいて、当該PCカードは、記憶媒体を備えた記憶装置であることを特徴するPCカード。

【請求項6】 請求項1～4に記載のPCカードにおいて、当該PCカードは、通信機能を前記外部機器に付加する通信装置であることを特徴とするPCカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、外部機器に着脱されるPCカードに係り、特に使用者の認証を行なうことのできるPCカードに関する。

【0002】

【従来の技術】近時、ポータブルPC（パーソナルコンピュータ）等が普及し、その拡張デバイスとしてPCカード等のカード型拡張デバイスが多用されている。これらの拡張デバイスはポータブルPC等に様々な機能を提供するものであり、例えば、半導体メモリやハードディスク等に情報を記憶するメモリデバイスとして機能するPCカードや、通信装置として機能するPCカード等が市販されている。

【0003】メモリデバイスの記憶容量は飛躍的に増大

しており、メモリデバイスとして機能するPCカード内に秘密保持を要する情報が格納される可能性が高くなってきている。また、通信装置として機能するPCカードを用いてネットワークに接続し、ポータブルPC等にて電子商取引や銀行取引の処理等を行ったりすることが多くなっている。即ち、ポータブルPC等において秘密保持を要する情報が増え、これらの情報がメモリデバイスに内包したPCカード内に格納されることが多くなっている。

【0004】ところで、PCカード等のカード型拡張デバイスは、ポータブルPC等に対して着脱が容易であり、かつ単体での携行に好適であるため、紛失や、第三者による誤用等の発生を完全に排除することは困難である。即ち、カード型拡張デバイスに格納された秘密保持を要する情報が、第三者に利用される可能性がある。このような事態を回避するために、カード型拡張デバイスがポータブルPC等の外部機器に装着された後に認証処理を行って、使用者が本人であるか否かの認証（以下、本人認証という）を行なうことが考えられる。

【0005】一般に、カードの使用者が本人であるか否かの認証を行う方法としては、磁気ストライプを有するカード（例えば、キャッシュカード）等においては磁気ストライプを読み取って当該カードに対応した暗証番号の入力を要求する方法や、認証データを記憶したICカード等においてはその認証データを読み取って鍵情報を作成し、認証を行う方法等が広く知られている。また、より高度なセキュリティの確保やクレジットカード等を用いたキャッシュレスサービス等の実現を目的とし、使用者の生体情報（例えば、指紋、音声等）を用いた本人認証を行う方法も提案されている。

【0006】

【発明が解決しようとする課題】しかしながら、従来のPCカードやその他のカードを用いる本人認証は、カードを外部機器に装着した後に、この外部機器内の処理装置によって本人認証処理を行わせるため、カードを装着してから認証完了までに時間が必要となり、迅速な認証処理を実現することができなかった。

【0007】特に、外部機器（PCカード等）のカードスロットにPCカードを差し込んで行う認証処理は、①ポータブルPCを起動し、PCカードが装着されたか否かの認識、②本人認証に用いる使用者の情報および基準情報の読み込み、③使用者の情報と基準情報との比較照合、といった手順となる。このような、認証方法では、認証処理を外部機器に担わせているため、手間の掛かった操作性の悪いものとなっていた。

【0008】本発明は、以上の事情に鑑みてなされたもので、本発明は、PCカードの使用に際し、使用者がPCカードを把持した段階で、本人認証を行うことができるPCカードを提供することを目的とする。

【0009】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の発明は、外部機器に着脱されるPCカードであって、コネクタを有する筐体部と、該筐体部の表面に設けられ、使用者が把持する把持部と、該把持部を使用者が把持したとき、使用者の生体情報を検出する生体情報検出手段と、前記生体情報検出手段で検出された生体情報に基づいて特定の使用者か否かの本人認証を行う認証処理手段と、前記生体情報検出手段及び認証処理手段を駆動するための電力を供給する内蔵電源と、を備えたことを特徴としている。

【0010】請求項2記載の発明は、前記筐体部が外部機器に装着されるとき、前記認証処理手段の認証結果に基づいて、当該PCカードを外部機器に対して動作許可状態又は動作禁止状態にすることを特徴としている。

【0011】請求項3記載の発明は、前記生体情報検出手段は、前記把持部に設けられ、該把持部を把持する使用者の指紋情報を検出することを特徴としている。

【0012】請求項4記載の発明は、請求項1または2に記載のPCカードにおいて、前記認証処理手段による本人認証が完了してから所定時間の間、認証結果を出力

【0013】請求項5記載の発明は、請求項1〜4に記載のPCカードにおいて、当該PCカードは、記憶媒体を備えた記憶装置であることを特徴としている。

【0014】請求項6記載の発明は、請求項1〜4に記載のPCカードにおいて、当該PCカードは、通信機能を前記外部機器に付加する通信装置であることを特徴としている。

【0015】

【発明の実施の形態】以下、本発明の好ましい実施形態について図面を参照しつつ説明する。

【0016】(1)実施形態

(1-1)PCカードの構成

図1ないし図3は、本発明に係るPCカードの一実施形態を示す図あり、本実施形態では、PCカードスタンダード形のものを例示する。

【0017】まず、図1の概略構成図に基づいてPCカード1の構成について説明する。PCカード1は、所定記憶容量の記憶媒体を有するメモリデバイスとして機能するものである。なお、本発明によるPCカード1は、メモリデバイスに限定される趣旨ではなく、通信装置として機能するもの、或いは他の拡張デバイスであってもよい。このPCカード1は、把持部2aを有する筐体部2と、生体情報検出手段(SCN)3と、マイクロコントローラ(MC)4と、メモリ(MEM)5と、バッテリー(BT)6と、コネクタ7とによって大略構成されている。そして、PCカード1は、図2に示すように、筐体部2がそのタイプに対応する所定形式のPCカードスロット9aを持つポータブルPC等の外部機器9に装着されるようになっている。

【0018】ここで、筐体部2は、PCカード1の外形をなし、この筐体部2には使用者がPCカード1を持ち易くする把持部2aが形成されている。また、把持部2aには、この把持部2aを把持する使用者の指紋情報を検出する生体情報検出手段3が装着されている。この生体情報検出手段3は、筐体部2の少なくとも片面側の所定位置(両面の異なる位置でもよい)で使用者の指紋情報を検出するものである。生体情報検出手段3は、カード把持時に把持部2aに密着した指の指紋だけが読取可能なように、公知のCCD(Charge Coupled Device: 電荷結合素子)等によって構成されている。また、生体情報検出手段3は、使用者の指紋を検出するのみでなく、使用者の把持状態を検知するスイッチを把持部2aに備え、使用者が把持部2aを把持したときに、マイクロホンで使用者の音声を読み込み、この音声进行分析して生体情報として検出してもよい。なお、スイッチは機械的なスイッチに限らず、例えば、把持部2aに圧力センサを設け、使用者のカード1を把持する圧力によってスイッチング動作を行ったり、筐体部2の先端に接触センサを設け、カードスロット側のシャッタを開いたときにスイッチング動作を行うようにして、スイッチの代用とすることも可能である。

【0019】マイクロコントローラ4及びメモリ5は、指紋情報に基づいて使用者が特定の使用者か否かの本人認証を行う認証処理を行うものである。このマイクロコントローラ4は、生体情報検出手段3で検出された指紋データからその指紋の特徴パターンを抽出する処理を実行する。また、マイクロコントローラ4は、後述する認証処理プログラムに従ってこの特徴パターンに基づいて認証を行う。また、メモリ5の所定領域には、認識処理を実行するための制御プログラムと、予め記憶した登録データ(特定の使用者の指紋の特徴パターンデータ等)が記憶されている。

【0020】具体的には、マイクロコントローラ4は、メモリ5に格納された制御プログラムに従って、予め記憶した登録データ(特定の使用者の指紋の特徴パターンデータ)をメモリ5の所定領域から読み出し、生体情報検出手段3で読み取った指紋情報について特徴抽出処理を行なった結果の指紋のパターンデータと比較照合する。この場合、読み取り範囲と登録パターンの範囲との関係は、例えば読み取り範囲を広く、登録パターンの範囲を狭くする。これにより、マイクロコントローラ4による比較照合は、読み取り範囲をサーチ領域とし、このサーチ領域内で指紋の登録パターンと類似のものを指紋の長さや間隔、形状等からサーチする、といった比較を行う。

【0021】その照合の結果、双方の指紋の特徴パターンが一致すると判定されれば本人である旨の認証結果に対応した信号をコネクタ7から出力し、認証完了後にPCカード1を所定の動作許可状態にする。この状態で、

PCカード1が外部機器9等に装着された場合には、このPCカード1は動作可能となる。一方、照合の結果、双方の指紋の特徴パターンが一致しなければ、本人でない旨の認証結果に対応した信号をコネクタ7から出力し、認証前の状態と同様の所定の動作禁止状態となる。この動作禁止状態では、PCカード1が外部機器9に接続されても外部機器9に全く応答せずに動作させないか、若しくは、その機能の一部に制限が加えられた状態となる（例えば、通信装置の発信動作や、ファイルシステム内の特定のファイルやディレクトリへのアクセスができなくなる等の状態となる）。ここにいう動作禁止状態とは、外部機器9等からPCカード1に対してアクセスができない状態である。また、外部機器9に動作禁止状態にあるPCカード1が装着された場合であっても、PCカード1の把持部2aを使用者が把持して生体情報が入力されたときには、即座にその生体情報（指紋情報）を読み取って前記認証処理を行うことも可能である。なお、指紋データの比較照合の方法は、例えば特開平10-312459号公報等に開示されている。

【0022】また、マイクロコントローラ4の内部には図示しないタイマ機構を有しており、使用者の把持による認証完了後に、一定の所定時間内に外部機器9への挿入（正常な接続状態となる装着）がなされない場合には、既に行なった認証結果を無効とすることにより、情報に対するセキュリティ性能を向上させるようにしている。

【0023】さらに、マイクロコントローラ4は、使用者がカードの所有者等である認証が完了した場合、所定の方式で暗号化した所定のユーザ識別コードやパスワード情報等をコネクタ7を介して外部機器9側に出力し、外部機器9側で使用者を認証させることも可能である。

【0024】コネクタ7は、筐体2の先端側（図2中の右側）に設けられたものであり、このコネクタ7は、例えばPCカード・スタンダード（PC Card Standard）形式に対応したものである。なお、コネクタ7は、これに限らず、携帯端末その他の外部情報機器との接続用のコネクタを構成できる汎用性の高い他形式のもの、例えばコンパクトフラッシュ・タイプII（Compact Flash Type II）に対応したものでよい。ここで、PCカード・スタンダードとは、JEIDA（Japan Electronics Industry Development Association：日本電子工業振興協会）と米国PCMCIA（Personal Computer Memory Card International Association）が共同で制定したPCカードの規格であり、厚さによって異なるタイプI、タイプII、タイプIII、タイプIV等がある。コンパクトフラッシュ（Compact Flash）・タイプは更に小型で、タイプIIは縦横が42.8×36.4、厚さが5.0(mm)である。このため、これらに対応したコネクタをコネクタ7に採用した場合には、PCカード1の小型化が容易となる。

【0025】（1-2）認証処理の動作

次に、PCカード1による認証処理の動作について、図3のフローチャートを参照しつつ説明する。

【0026】上述のように構成された本実施形態においては、使用者がPCカード1の筐体部2の把持部2aを把持すると、バッテリー6の電力がマイクロコントローラ4、生体情報検出手段3等に供給され、これらを駆動して認証処理が開始される。マイクロコントローラ4は、生体情報検出手段3によって使用者の指紋情報の読み取りを行う（ステップS1）。

【0027】次いで、マイクロコントローラ4は、生体情報が入力されたか否か、即ちPCカード1の筐体部2の把持部2aに密着した使用者の指紋が入力されたか否かをチェックし（ステップS2）、指紋情報が入力されていれば（ステップS2：YES）、その指紋データに基づいてその指紋の特徴の抽出処理が実行される（ステップS3）。また、これと同時に、或いはこれに先立って、マイクロコントローラ4は、登録された使用者の指紋の特徴データをメモリ5から読み出す（ステップS4）。一方、マイクロコントローラ4は、指紋情報が入力されない場合（ステップS2：NO）には、使用者がカード把持してから所定時間が経過したか否かがチェックされ（ステップS1.1）、所定時間が経過していなければ、再度、指紋情報の入力とそのチェックがなされる（ステップS1、S2）。

【0028】次いで、マイクロコントローラ4は、今回入力された指紋の特徴と登録された使用者の指紋の特徴とが一致するかを比較照合し（ステップS5）、双方の特徴が一致するか否かが判定される（ステップS6）。

【0029】そして、マイクロコントローラ4は、その処理結果に応じて、双方の指紋の特徴が一致する場合（ステップS6：YES）には、カード装着後にPCカード1の動作が可能な所定の動作許可状態とし（ステップS7）、双方の指紋の特徴が一致しない（ステップS6：NO）場合には、カード装着後にPCカード1の動作ができない動作禁止状態にする（ステップS10）。なお、動作禁止状態において、未認証により動作禁止状態である旨の信号を外部機器9側に向けて報知する信号出力を行なうようにしてもよい。

【0030】また、ステップS7で動作許可状態になると、マイクロコントローラ4は、その後の所定時間内にPCカード1が外部機器9のPCカードスロット9aに挿入されて、正常に接続されたか否かをチェックする（ステップS8）。所定時間内にPCカード1がPCカードスロット9aに挿入された場合（ステップS8：YES）には、マイクロコントローラ4は、所定時間毎にPCカード1が外部機器9のPCカードスロット9aから外されたか否かをチェックする（ステップS9）。一方、PCカード1が外部機器9のPCカードスロット9aに正常に挿入されないまま所定時間が経過した場合

(ステップS8; NO)、または正常な挿入後にPCカード1が外された場合(ステップS9; YES)、マイクロコントローラ4は、その時点でPCカード1を動作禁止状態にする(ステップS10)。

【0031】(1-3)実施形態の効果

このように本実施形態においては、使用者がPCカード1の把持部2aを把持した段階で認証処理を行うため、外部機器9にPCカード1が装着するときには、本人の認証が確認でき、従来のようにPCカードを外部機器(例えば、ポータブルPC)に装着した後に面倒な認証処理のためのパスワード入力等を行ったりする必要がなくなる。即ち、本実施形態では、カード装着に先立ってPCカード1を使用者が把持することにより、迅速な本人認証を行うことができ、装着後に認証処理を行う必要がなくなる。

【0032】従って、PCカード1は、メモリカードに限らず、他のストレージ系PCカードであっても、このPCカード1内の記憶情報を保護するプロテクト機能を付加しながら、PCカード1に対する情報の迅速な書き込み/読み出しが可能となる。

【0033】また、本実施形態においては、マイクロコントローラ4にタイマ機能を持たせて、認証後の一定時間内に正常な接続がなされないときは認証結果を無効にするようにしているので、PCカード1のセキュリティ性能をより向上させることができる。

【0034】さらに、外部機器9にPCカード1が装着された後は、このPCカード1は外部機器9の一部として管理され、外部機器9の使用者の認証処理等に応じて使用される。勿論、拡張デバイスとしてのPCカード1にパスワードを設定しておき、電源投入後の最初の使用時にパスワード入力を要求したり、カード外端面部(挿入方向後端)のPCカード1若しくは外部機器9側のマイクロホンで入力した音声の特徴を抽出することで再度認証を行なうことも可能である。

【0035】(2)変形例

(2-1)変形例1

変形例1によるPCカード12は、生体情報検出手段をカード両面(表裏両面)の把持部12aと幅方向両側の側面12bと後端面12cとに、それぞれに配置された点にある。PCカード12には、その起端側を覆うように、カード両面(表面及び裏面)の把持部12aと、両側の把持部12bと、起端面の把持部12cとによって形成されている。そして、これらの把持部のうち複数の箇所に、生体情報検出手段による指紋参照窓等が配置されている。

【0036】起端面の把持部12cは、専ら挿入完了時に親指等で押圧される部分であり、カード把持時に単独で指に接し難いが、PCカード12の起端面以外の他の面と同時に把持され得るものであり、本発明にいう把持

部に含まれる。各把持部12a、12b、12cにおける指紋参照窓等の形状や個数等が任意であることはいうまでもない。PCカード12の両面に形状の異なる指紋参照窓を設けたり、他種類の生体情報入力部(例えば音声入力部)を併設したりすることも可能である。

【0037】(2-2)変形例2

前記各実施形態では、PCカード1をメモリデバイスとして用いた場合を例示したが、通信装置等のモデム機能を持つPCカードであっても、そのID格納メモリ、その他のメモリに使用者の指紋の特徴データを記憶させておき、マイクロコントローラ4による認証処理を行なうことも可能である。従って、PCカード1が、通信機能を備えたPCカードであれば、このPCカード1による通信回線の不正使用を防止しながら迅速な回線接続ができる。

【0038】

【発明の効果】本発明によれば、外部機器へのPCカードの装着に先立って、PCカードを使用者が把持することにより、本人認証をPCカード自体で迅速に完了することができる。これにより、装着後の本人認証の処理を省略することができる。この結果、PCカードがメモリデバイスとして機能するものであれば、このカード内の記憶情報を保護するプロテクト機能を付加しながら、迅速な書き込み/読み出しができ、PCカードが通信装置として機能するものであれば、このカードによる通信回線の不正使用を防止しながら迅速な回線接続を可能とする。

【図面の簡単な説明】

【図1】 本発明の実施形態に係るPCカードの概略構成を示すブロック図である。

【図2】 同実施形態のPCカードの把持部周辺を示す上面図である。

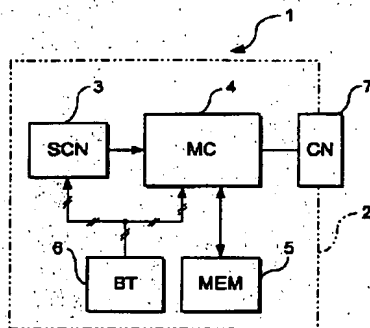
【図3】 同実施形態に係るPCカードの認識処理手順を説明するフローチャートである。

【図4】 本発明の変形例に係るPCカードの把持部周辺の外観図で、(a)はその平面図、(b)はその側面図である。

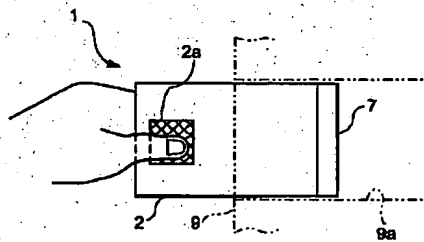
【符号の説明】

- 1、12・・・PCカード
- 2・・・筐体部
- 2a、12a、12b・・・把持部
- 12c・・・後端面(把持部)
- 3・・・生体情報検出手段(指紋入力手段)
- 4・・・マイクロコントローラ(認証処理手段)
- 5・・・メモリ
- 6・・・バッテリー(内蔵電源)
- 7・・・コネクタ
- 9・・・外部機器
- 9a・・・PCカードスロット

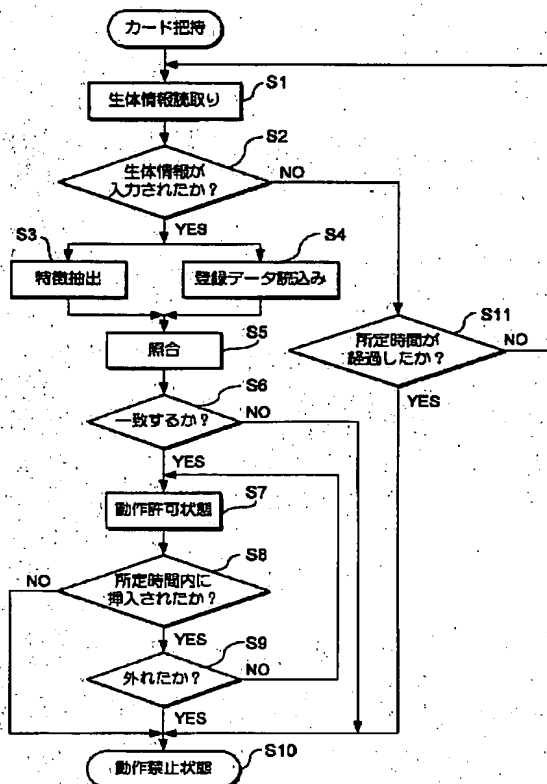
【図1】



【図2】



【図3】



【図4】

